ON ARITHMETIC PROGRESSIONS IN $A + B + C$

KEVIN HENRIOT

ABSTRACT. Our main result states that when A, B, C are subsets of $\mathbb{Z}/N\mathbb{Z}$ of respective densities α, β, γ, the sumset $A + B + C$ contains an arithmetic progression of length at least $e^{c(\log N)^c}$ for densities $\alpha \geqslant (\log N)^{-2+\varepsilon}$ and $\beta, \gamma \geqslant e^{-c(\log N)^c}$, where c depends on ε. Previous results of this type required one set to have density at least $(\log N)^{-1+o(1)}$. Our argument relies on the method of Croot, Łaba and Sisask to establish a similar estimate for the sumset $A + B$ and on the recent advances on Roth's theorem by Sanders. We also obtain new estimates for the analogous problem in the primes studied by Cui, Li and Xue.

1. INTRODUCTION

Let A and B be subsets of a cyclic group $\mathbb{Z}/N\mathbb{Z}$ of density α and β. The problem of finding long arithmetic progressions in $A+B$ has a rich history starting with the striking result of Bourgain [2]: the sumset $A + B$ always contains an arithmetic progression of length at least $e^{c(\alpha\beta\log N)^{1/3}}$ provided the densities satisfy $\alpha\beta \geqslant (\log N)^{-1+o(1)}$ (and the progression is non-trivial in this range: this will always be the case later when we specify a range of density). Major progress was made by Green [11] who showed that, under the same condition on densities, the progression could be taken as large as $e^{c(\alpha\beta\log N)^{1/2}}$. Sanders [18] later found a very different proof of Green's theorem and yet a third and relatively simple proof was provided recently by Croot, Łaba and Sisask [6].

For fixed densities α and β, the progression found has length $e^{c\sqrt{\log N}}$ and this has not been improved to date, while a negative result of Ruzsa [17] says that one cannot do better than $e^{c(\log N)^{2/3+\varepsilon}}$. However when densities are allowed to decrease with N, a remarkable result was obtained recently by Croot, Łaba and Sisask [6]. Improving on a first result of Croot and Sisask [8], they showed that the sumset $A + B$ contains an arithmetic progression of size at least $e^{c(\alpha\log N)^{1/2}/(\log 2\beta^{-1})^{3/2}}$ in a range $\alpha(\log \frac{2}{\beta})^{-5} \geqslant C(\log N)^{-1+o(1)}$. While the theorems of Bourgain and Green require one set to have density at least $(\log N)^{-1/2+o(1)}$, this allows for both sets to have density as low as $(\log N)^{-1+o(1)}$; further, one set may even have exponentially small density $e^{-C(\log N)^{1/5+o(1)}}$.

The analogous problem for three-fold sumsets was first studied by Freiman, Halberstam and Ruzsa [10], who established that the sumset $A+A+A$ contains a much longer progression: indeed of length at least $N^{c\alpha^3}$. Green [11] extended this to $N^{c\alpha^{2+o(1)}}$ and Sanders [18] to $N^{c\alpha^{1+o(1)}}$, however all of these results required $\alpha \geqslant (\log N)^{-1/2+o(1)}$. By contrast the best result known for four sets or more, due to Sanders [22], says that the sumset $A + A + A + A$ contains an arithmetic progression of length $N^{c/(\log 2\alpha^{-1})^4}$ when $\alpha \geqslant e^{-C(\log N)^{1/5}}$: in that case all the summands may be rather sparse. In this work we investigate in detail the sumset $A + B + C$, aiming at establishing results valid for sparse sets B and C and in a large range of α.

We now turn to the precise results[1], starting with the theorem of Croot, Laba and Sisask [6], which constitutes the state-of-the-art on arithmetic progressions in $A + B$.

Theorem 1.1 (Croot, Laba, Sisask)**.** *Suppose that A and B are subsets of $\mathbb{Z}/N\mathbb{Z}$ of respective densities α and β. Then there exists an absolute constant $c > 0$ such that $A + B$ contains an arithmetic progression of length at least*

$$e^{c(\alpha \log N)^{1/2}(\log 2\beta^{-1})^{-3/2}} \quad \text{if} \quad \alpha\left(\log \frac{\log N}{\beta}\right)^{-5} \geqslant (c \log N)^{-1}.$$

In the case of three summands, the best bounds known are due to Sanders [18].

Theorem 1.2 (Sanders)**.** *Suppose that A, B, C are subsets of $\mathbb{Z}/N\mathbb{Z}$ of respective densities α, β, γ. Then there exists an absolute constant $c > 0$ such that $A+B+C$ contains an arithmetic progression of length at least*

$$N^{c(\alpha\beta\gamma)^{1/3}} \quad \text{if} \quad (\alpha\beta\gamma)^{1/3} \geqslant (c \log N)^{-1/2}(\log \log N)^{1/2}.$$

Cui, Li and Xue [9] also recently studied the analogous problem for subsets of the primes. We let $\log_k$ denote the logarithm iterated k times below.

Theorem 1.3 (Cui, Li, Xue)**.** *Suppose that A is a subset of the primes less than N of size $\alpha N/\log N$. Then there exist absolute positive constants c, c_0, c_1 such that $A+A+A$ contains an arithmetic progression of length at least*

$$N^{c\alpha^2/(\log 2\alpha^{-1})} \quad \text{if} \quad \alpha \geqslant (\log_3 N)^{-c_0},$$
$$N^{c\alpha^4/(\log 2\alpha^{-1})} \quad \text{if} \quad \alpha \geqslant (\log N)^{-c_1}.$$

Their argument relies on a clever combination of Green's [12] and Helfgott and de Roton's [15] restriction theorems for primes with Green's [11] theorem on $A + A + A$, modified to obtain arithmetic progressions whose elements all have a certain number

---

[1]We assume that $N \geqslant 1 + \exp(e^e)$ throughout this introduction to alleviate logarithmic notations.

of representations as a sum of three elements of A. For lack of an existing expression, we call **counting lemma** any lower bound on this number of representations, here and throughout the article. Motivated by the application to the problem of sumsets of primes we set out, as a secondary objective, to provide counting lemmas in all our estimates; this is not essentially difficult although it requires some care in the computations.

We now introduce our results. We start with a simple observation which is that the almost-periodicity results of Croot, Laba and Sisask [6] imply a version of Theorem 1.2 which allows for two sets out of three to be sparse, with density as small as $e^{-c(\log N)^{1/5}}$.

Theorem 1.4. *Suppose that A, B, C are subsets of $\mathbb{Z}/N\mathbb{Z}$ of respective densities α, β, γ. Then there exists an absolute constant $c > 0$ such that $A + B + C$ contains an arithmetic progression of length at least*

$$N^{c\alpha^2/\log^4(2/\alpha\beta\gamma)} \quad if \quad \alpha\big(\log \tfrac{2}{\alpha\beta\gamma}\big)^{-5/2} \geqslant (c\log N)^{-1/2}$$

such that each element of the progression has at least $\frac{1}{2}\alpha\beta\gamma N^2$ representations as a sum $x + y + z$ with $(x, y, z) \in A \times B \times C$.

While the dependency on densities β and γ in Theorem 1.4 is satisfactory, the density α is still required to be at least $(\log N)^{-1/2}$, and the arithmetic progression is shorter than that of Theorem 1.2 when $\alpha = \beta = \gamma$. To overcome these limitations we turn to the argument of Sanders [18] to prove Theorem 1.2. The proof there is based on a density-increment strategy, which builds on that introduced by Bourgain [3] in the context of Roth's theorem [16]. Sanders' recent breaktrough [20] in the latter problem introduced very powerful new techniques, and these allow us to revisit the argument of [18] so as to obtain the following.

Theorem 1.5. *Suppose that A, B, C are subsets of $\mathbb{Z}/N\mathbb{Z}$ of respective densities α, β, γ. Then there exists an absolute constant $c > 0$ such that $A + B + C$ contains an arithmetic progression of length at least*

$$N^{c\alpha/\log^5(2/\alpha\beta\gamma)} \quad if \quad \alpha\big(\log \tfrac{2}{\alpha\beta\gamma}\big)^{-7} \geqslant (c\log N)^{-1}$$

such that each element of the progression has at least $e^{-(c\alpha)^{-1}\log^7(2/\alpha\beta\gamma)}N^2$ representations as a sum $x + y + z$ with $(x, y, z) \in A \times B \times C$.

Note that the density of each set may now be as low as $(\log N)^{-1+o(1)}$, and that we may take two sets to be very sparse as before. A result of this kind also follows from Theorem 1.1, since an arithmetic progression in $A + B$ is always contained, up to translation, in $A + B + C$; however the arithmetic progression obtained in this way is

shorter than the one given by Theorem 1.5, unless γ is extremely small[2]. Surprisingly, the counting lemma of Theorem 1.5 is quite a lot weaker than that of Theorem 1.4: this is due to the use of an iterative argument which at each step places the sets A, B, C in a certain Bohr set, whose size decreases as we iterate.

By using a generalization by Bloom [1] of the Katz-Koester transform of Sanders [20] to three or more sets we are able to go one step further in the range of density, however this time the loss in the counting lemma is substantial.

Theorem 1.6. *Let $\varepsilon \in (0, 1)$ be a parameter and suppose that A, B, C are subsets of $\mathbb{Z}/N\mathbb{Z}$ of respective densities α, β, γ. Then there exists an absolute constant $c > 0$ such that $A + B + C$ contains an arithmetic progression of length at least*

$$\exp\left(c\alpha^{1/4}(\varepsilon \log N)^{1/2}\left(\log \tfrac{2}{\alpha\beta\gamma}\right)^{-7/2}\right) \quad \text{if} \quad \alpha\left(\log \tfrac{2}{\alpha\beta\gamma}\right)^{-14} \geqslant (c\varepsilon \log N)^{-2}$$

such that each element of the progression has at least $N^{2-\varepsilon}$ representations as a sum $x + y + z$ with $(x, y, z) \in A \times B \times C$.

Note that the progression obtained in this way is in fact longer than that of Theorem 1.5 in the range $(\log N)^{-1+o(1)} \leqslant \alpha \leqslant (\log N)^{-2/3+o(1)}$ when, say, $\alpha = \beta = \gamma$ and $\varepsilon \asymp 1$. Finally, we mention two applications of the above results to the analogous problem in the primes. First, since Theorem 1.5 comes with a counting lemma, its conclusion may be inserted into the original argument of Cui, Li and Xue [9] to derive two new estimates, which complement Theorem 1.3.

Theorem 1.7. *Suppose that A is a subset of the primes less than N of size $\alpha N/\log N$. Then there exist absolute positive constants c, c_2, c_3 such that $A + A + A$ contains an arithmetic progression of length at least*

$$N^{c\alpha/(\log 2\alpha^{-1})^5} \quad \text{if} \quad \alpha \geqslant (\log_4 N)^{-c_2},$$
$$N^{c\alpha^2/(\log 2\alpha^{-1})^5} \quad \text{if} \quad \alpha \geqslant (\log_2 N)^{-c_3}.$$

Secondly, Theorem 1.6, thanks to its longer density range, allows us to find long arithmetic progressions in $A + A + A$ for a dense subset A of the primes on grounds of density alone, i.e. without appealing to restriction theorems for the primes. This is mostly of conceptual interest, since our argument is also quite involved, relying heavily on methods from [20]. We record below the estimate that might be obtained from Theorem 1.6, by observing that the primes have asymptotic density $(\log N)^{-1}$ in the first N integers and with the usual Freiman embedding.

---

[2]For e.g. $\alpha \asymp \beta \asymp (\log N)^{-\varepsilon}$ and $\gamma \asymp e^{-C(\log N)^{(1-\varepsilon)/7}}$, Theorem 1.1 yields a longer progression.

Corollary 1.8. *Suppose that A is a subset of the primes less than N of size $\alpha N / \log N$. Then there exists an absolute positive constant c such that $A + A + A$ contains an arithmetic progression of length at least*

$$e^{c(\alpha \log N)^{1/4} (\log \log N)^{-7/2}} \quad \text{if} \quad \alpha \geqslant (\log N)^{-1} (\log \log N)^{14}.$$

By comparison the constant c_1 in Theorem 1.3 is $1/45$ in the original argument of [9]. The arithmetic progression given by this corollary is however shorter than that of Theorems 1.3 and 1.7 in the ranges prescribed there.

We make two last remarks about the shape of the above bounds. The first is that in Theorems 1.4, 1.5 and 1.6, one may assume $\alpha \geqslant \beta \geqslant \gamma$ without loss of generality, and that under this assumption one may replace logarithmic terms $\log \frac{2}{\alpha\beta\gamma}$ by $\log \frac{2}{\beta\gamma}$ there. Secondly, we note that Theorems 1.4 to 1.7 and Corollary 1.8 are non-trivial if and only if N is larger than an absolute constant.

At this point we should also remark that arithmetic progressions may be obtained for sets much sparser than the ones considered above by a combinatorial method of Croot, Ruzsa and Schoen [7], recently generalized in [14], although the results there take a rather different form. Indeed while the Fourier analytic methods used here typically find progressions of length $e^{(\log N)^c}$ in a range of density $\alpha \geqslant (\log N)^{-\delta}$, these combinatorial methods produce shorter progressions, of size $(\log N)^c$, for a larger range of density $\alpha \geqslant N^{-\delta}$.

The article is now organized as follows. Section 2 is devoted to notations and Section 3 is there to recall relevant facts about Bohr sets. The proof of Theorem 1.4 is given in Section 4, and in Section 5 we collect a number of facts on the density-increment strategy which are then used to give the proof of Theorems 1.5 and 1.6 in Section 6. Finally the estimates of Theorem 1.7 and Corollary 1.8 are derived in Section 7, and comparisons with results on Roth's theorem are drawn in Section 8.

2. NOTATIONS

Here we take a moment to introduce our notations. These are mostly standard up to the choice of normalizations.

General setting. For the rest of the article we fix an integer $N \geqslant 2$ and we write $G = \mathbb{Z}/N\mathbb{Z}$. It is clear however that our results are only meaningful when densities vary with N and when N is large: one should think of N as such.

Functions. For a subset X of G and $x \in G$, we define the averaging operator over X, and the operator of translation by x on functions $f : G \to \mathbb{C}$, respectively, by

$$\mathbb{E}_{x \in X} f(x) = \frac{1}{|X|} \sum_{x \in X} f(x) \quad \text{and} \quad \tau_x(f)(u) = f(u + x) \quad \text{for } u \in G.$$

We also occasionally use the identity operator I defined by $If = f$. For any $p \geqslant 1$ we define the L^p-norm of a function f on G by

$$\|f\|_{L^p} = \left(\mathbb{E}_{x \in G} |f(x)|^p \right)^{1/p}.$$

We let $\|f\|_\infty = \sup_{x \in G} |f(x)|$ denote the uniform norm of f over G. The scalar product and the convolution of two functions f, g are defined respectively by

$$\langle f, g \rangle_{L^2} = \mathbb{E}_{x \in G} f(x) \overline{g(x)}$$

$$\text{and} \quad f * g(x) = \mathbb{E}_{y \in G} f(y) g(x - y) \qquad (x \in G).$$

We also let $f^{(\ell)} = f * \cdots * f$ denote the convolution of f with itself ℓ times.

Fourier analysis on $\mathbb{Z}/N\mathbb{Z}$. We let $\widehat{G}$ denote the dual group of G, that is, the set of homomorphisms $\gamma : G \to \mathbb{T}$, where $\mathbb{T}$ denotes the unit circle $\{\omega \in \mathbb{C} : |\omega| = 1\}$. We define the Fourier transform $\widehat{f}$ of a function $f : G \to \mathbb{C}$ by

$$\widehat{f}(\gamma) := \mathbb{E}_{x \in G} f(x) \overline{\gamma(x)} \qquad (\gamma \in \widehat{G}).$$

The three basic formulæ of Fourier analysis then read as follows:

(Inversion) $\qquad\qquad f(x) = \sum_{\gamma \in \widehat{G}} \widehat{f}(\gamma) \gamma(x),$

(Parseval) $\qquad\qquad \langle f, g \rangle_{L^2} = \sum_{\gamma \in \widehat{G}} f(\gamma) \overline{g(\gamma)},$

(Convolution) $\qquad\qquad \widehat{f * g}(\gamma) = \widehat{f}(\gamma) \widehat{g}(\gamma).$

For functions $g, h \colon \widehat{G} \to \mathbb{C}$ we also write

$$\|g\|_{\ell^p} = \left(\sum_{\gamma \in \widehat{G}} |\widehat{g}(\gamma)|^p \right)^{1/p} \quad \text{and} \quad \langle g, h \rangle_{\ell^2} = \sum_{\gamma \in \widehat{G}} g(\gamma) \overline{h(\gamma)}.$$

Finally, for a real number $\eta > 0$ we define the η-spectrum of a function $f \colon G \to \mathbb{C}$ by

$$\mathrm{Spec}_\eta(f) = \{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geqslant \eta \|f\|_{L^1}\}.$$

Characteristic functions and densities. We let m_G denote the uniform measure on G defined by $m_G(X) = |X|/|G|$ for $X \subset G$. More generally when A is a subset of G we let m_A denote the uniform measure on A defined by $m_A(X) = |X \cap A|/|A|$ for $X \subset G$. We also define the normalized characteristic function of a subset A of G by

$$\mu_A = m_G(A)^{-1} 1_A$$

so that $\|\mu_A\|_{L^1} = 1$; note also the useful identity $1_A * \mu_B(x) = m_{-B}(A - x)$. When B is a subset of G we say that $A \subset B$ has relative density α when $|A| = \alpha|B|$, that is, when $m_B(A) = \alpha$. Note the composition identity $m_G(A) = m_B(A)m_G(B)$.

Asymptotic notations. We let c and C denote absolute positive constants which may take different values at each occurrence. We also make occasional use of Landau's and Vinogradov's asymptotic notations: for two non-negative functions f and g, we let $f = O(g)$ or $f \ll g$ indicate the fact the $f \leqslant Cg$ for some constant $C > 0$, and $f = \Omega(g)$ or $f \gg g$ indicate that $f \geqslant cg$ for some constant $c > 0$. We write $f \asymp g$ when $f \ll g$ and $f \gg g$.

3. Preliminaries on Bohr sets

Bohr sets are now a standard tool of additive combinatorics. The definition and terminology we use follows Sanders [20, 21]. We also recall the fundamental properties of these sets which will be needed for our work.

Definition 3.1 (Bohr set). *For a set of characters $\Gamma \subset \widehat{G}$ and a real number $\delta > 0$ we let*

$$B(\Gamma, \delta) = \{x \in G : |1 - \gamma(x)| \leqslant \delta \ \ \forall \gamma \in \Gamma\}$$

*be the Bohr set of **frequency set** Γ and **radius** δ. We define $d = |\Gamma|$ to be the **dimension** of this Bohr set.*

Note that $\gamma(x) \in \mathbb{T}$ and therefore $|1 - \gamma(x)| \leqslant 2$ for every $x \in G$ and $\gamma \in \widehat{G}$, so that the definition is only interesting for $\delta \leqslant 2$. We will often denote a Bohr set simply by the letter B, with associated parameters[3] Γ, δ, d. We also define the **dilate** of B by a factor ρ by $B_\rho = B(\Gamma, \delta)_\rho := B(\Gamma, \rho\delta)$. Finally we say that B' is a **sub-Bohr-set** of B, and we write $B' \leqslant B$, when $\Gamma \subset \Gamma'$ and $\delta' \leqslant \delta$.

---

[3] There is a slight abuse of notations in doing so, as the physical set B may be the same for different frequency sets and radii: one should formally think of B as a triple (B, Γ, δ).

We now recall a bound on the growth of Bohr sets. The proof can be found in [24, Lemma 4.20]; small adjustments[4] have to be made to fit our slightly different definition of a Bohr set.

Lemma 3.2 (Doubling ratio of Bohr sets). *Suppose that B is a Bohr set. Then*

$$m_G(B_{1/2}) \geqslant 7^{-d} m_G(B).$$

We record an immediate consequence of this bound.

Lemma 3.3 (Growth of Bohr sets). *Suppose that B is a Bohr set and $\rho \in (0,1]$. Then*

$$m_G(B_\rho) \geqslant e^{-6d \log 2\rho^{-1}} m_G(B).$$

Observing that $B = B(\Gamma, 2)_{\delta/2}$ this in turn gives the following.

Lemma 3.4 (Size of Bohr sets). *Suppose that B is a Bohr set of radius $\delta \leqslant 2$. Then*

$$m_G(B) \geqslant e^{-6d \log 4\delta^{-1}}.$$

One essential fact about Bohr sets is that they support a lot of arithmetic structure. A simple illustration of this principle is given by the following easy consequence of Dirichlet's theorem on simultaneous approximation [23, Theorem II.1A].

Lemma 3.5 (Arithmetic progression in a Bohr set). *Let B be a Bohr set of radius $\delta < \pi$. Then B contains an arithmetic progression of size at least $(1/2\pi)\, \delta N^{1/d}$.*

We now recall the notion of regularity of Bohr sets which is of crucial importance for the proof of Theorems 1.5 and 1.6. This is not needed for the proof of Theorem 1.4, therefore the reader only interested in that result may very well skip the following discussion.

Bourgain [3] introduced the notion of regular Bohr sets in the context of Roth's theorem. In that situation one often needs to work with Bohr sets on different scales, and it is therefore desirable that the size of dilates $B_{1+\rho}$ vary continuously with ρ.

---

[4]Let $e(x) = e^{2i\pi x}$ and write characters $\gamma : G \to \mathbb{T}$ as $\gamma = e(\omega)$, where $\omega : G \to \mathbb{R}/\mathbb{Z}$. In [24] a Bohr set of frequency set Γ and radius δ is defined as $\tilde{B}(\Gamma, \delta) = \{x : |\omega(x)| \leqslant \delta \ \ \forall \omega \in \Gamma\}$, whereas here it is defined as $B(\Gamma, \delta) = \{x : |1 - e(\omega(x))| \leqslant \delta \ \ \forall \omega \in \Gamma\}$. The covering argument used in the proof of Lemma 4.20 of [24] may however be adjusted via the elementary inclusions

$$\{\omega : |1 - e(\omega)| \leqslant 4\delta\} \subset \{\omega : |\omega| \leqslant \delta\} \subset \{\omega : |1 - e(\omega)| \leqslant 2\pi\delta\}.$$

Definition 3.6 (Regular Bohr set). *Let C_0 be an absolute constant. A Bohr set B is said to be **regular** for C_0 if*

$$(3.1) \qquad 1 - C_0|\rho|d \leqslant \frac{|B_{1+\rho}|}{|B|} \leqslant 1 + C_0|\rho|d \qquad (0 < |\rho| < \tfrac{1}{C_0 d}).$$

An essential observation of Bourgain [3] is that one may always ensure the regularity of a Bohr set up to dilation by a constant factor.

Lemma 3.7 (Existence of regular Bohr sets). *There exists an absolute constant C_0 such that for **every** Bohr set B, there exists $\kappa \in [1/2, 1)$ such that B_κ is regular for C_0.*

The proof of this result can now be found in many places and we refer e.g. to Proposition 3.5 of [19]. From now on we fix C_0 and we simply say that a Bohr set B satisfying (3.1) is regular. The regularity property allows for a very useful averaging lemma, first formalized by Bourgain as Lemma 3.16 of [3]. The version we record below is closest to Lemma 4.2 of [13]; it says that Bohr sets are roughly invariant under translation by, or averaging over, elements of a smaller Bohr set.

Lemma 3.8 (Regularity averaging lemma). *Suppose that B is a regular Bohr set and let $x \in G$ and $\lambda : G \to \mathbb{C}$ with $\|\lambda\|_{L^1} = 1$. Then*

$$\|\mu_{x+B} - \mu_B\|_{L^1} \leqslant C_1 \rho d \qquad \qquad if \quad x \in B_\rho,$$
$$\|\mu_B * \lambda - \mu_B\|_{L^1} \leqslant C_1 \rho d \qquad \qquad if \quad \mathrm{Supp}(\lambda) \subset B_\rho,$$

provided $\rho \leqslant \frac{1}{C_0 d}$ and where $C_1 = 2C_0$.

Proof. Observe that $\|\mu_{x+B} - \mu_B\|_{L^1} = \frac{1}{|B|} \sum_{y \in G} |1_{x+B}(y) - 1_B(y)|$ and that 1_B and 1_{x+B} are equal on $B_{1-\rho}$ and outside $B_{1+\rho}$. Therefore $\|\mu_{x+B} - \mu_B\|_{L^1} \leqslant \frac{1}{|B|}(|B_{1+\rho}| - |B_{1-\rho}|)$ and the first bound follows from (3.1). Summing over x with weights $\lambda(x)$ and applying the triangle inequality yields the second estimate. $\qquad\square$

4. The Croot-Laba-Sisask approach

The aim of this section is to prove Theorem 1.4. This result is a rather direct consequence of Theorem 7.1 of [6] due to Croot, Laba and Sisask, which says that the set of almost-periods of a convolution is guaranteed to contain a large Bohr set. The proof of this theorem relies on a combination of the Croot-Sisask lemma [8] and Chang's spectral lemma [5, Lemmas 3.1 and 3.4]; this combination was first exploited by Sanders in [22, 20]. For our purpose we only need the following special case.

Lemma 4.1 (Bohr-almost-periodicity of convolutions). *Let $p \geqslant 2$ and $\theta \in (0,1)$ be a pair of parameters. Suppose that A_1, A_2 are subsets of $\mathbb{Z}/N\mathbb{Z}$ of respective densities α_1, α_2. Then there exists a Bohr set B such that*

$$\|1_{A_1} * \mu_{A_2} - \tau_x 1_{A_1} * \mu_{A_2}\|_{L^p} \leqslant \theta \alpha_1^{1/p} \qquad (x \in B)$$

with dimension and radius satisfying

$$d \leqslant Cp\theta^{-2}(\log \tfrac{2}{\theta\alpha_1\alpha_2})^3,$$
$$\delta \geqslant c(\theta\alpha_1\alpha_2/p)^C.$$

Proof. Apply Theorem 7.1 of [6] with $A = A_2$, $B = A_1$ and $S = G$, with doubling constants $K_1 = 2/\alpha_2$ and $K_2 = 2/\alpha_1$, and with $\varepsilon = \theta$. This yields a parameter

$$\delta' = c\theta\alpha_2^{1/2}\alpha_1^{1/p-1/2} \geqslant c\theta\alpha_2^{1/2}$$

and a Bohr set of dimension at most

$$d \leqslant Cp\theta^{-2}(\log 2/\delta')^2(\log 2/\alpha_2) \leqslant Cp\theta^{-2}\big(\log \tfrac{2}{\theta\alpha_1\alpha_2}\big)^3$$

and radius

$$\delta = \delta'/d \geqslant cp^{-1}\theta^3\alpha_2^{1/2}\big(\log \tfrac{2}{\theta\alpha_1\alpha_2}\big)^{-3} \gg (\theta\alpha_1\alpha_2/p)^4$$

satisfying the desired almost-periodicity property. The bound on δ might seem less crude once we notice that the lower bound of Lemma 3.4 on $\log m_G(B)$ depends linearly on d and $\log 2\delta^{-1}$. We have also been somewhat imprecise in handling logarithmic terms, so as not to needlessly clutter the main estimates: indeed these terms have little bearing on the quality of the final results. $\square$

From Lemma 4.1 we first obtain a result slightly more general than Theorem 1.4 which finds a translate of a Bohr set in a sumset. We follow the proof of the similar Theorem 1.7 on p. 1380 of [8], relying on little more than an elementary identity of convolutions.

Proposition 4.2. *Suppose that A_1, A_2, A_3 are subsets of $\mathbb{Z}/N\mathbb{Z}$ of respective densities $\alpha_1, \alpha_2, \alpha_3$. Then there exists $z \in G$ and a Bohr set B with*

$$d \leqslant C\alpha_1^{-2}\big(\log \tfrac{2}{\alpha_1\alpha_2\alpha_3}\big)^4$$
$$\delta \geqslant c(\alpha_1\alpha_2\alpha_3)^C$$

such that $1_{A_1} * 1_{A_2} * 1_{A_3}(y) \geqslant \frac{1}{2}\alpha_1\alpha_2\alpha_3$ for every $y \in z + B$.

Proof. Apply Lemma 4.1 to A_1 and A_2 with parameters p and θ to be determined later. This yields a Bohr set B with dimension $d \leqslant Cp\theta^{-2}\left(\log\frac{2}{\theta\alpha_1\alpha_2}\right)^3$ and radius $\delta \geqslant c(\theta\alpha_1\alpha_2/p)^C$ such that

$$(4.1) \qquad \|(I - \tau_x)1_{A_1} * \mu_{A_2}\|_{L^p} \leqslant \theta\alpha_1^{1/p} \qquad (x \in B).$$

Let $z \in G$ and $x \in B$ and observe that

$$1_{A_1} * \mu_{A_2} * \mu_{A_3}(z) - 1_{A_1} * \mu_{A_2} * \mu_{A_3}(z + x) = \langle (I - \tau_x)1_{A_1} * \mu_{A_2}, \tau_{-z}\mu_{-A_3}\rangle_{L^2}.$$

Applying successively Hölder's inequality and (4.1) we have therefore

$$|1_{A_1} * \mu_{A_2} * \mu_{A_3}(z) - 1_{A_1} * \mu_{A_2} * \mu_{A_3}(z + x)| \leqslant \|(I - \tau_x)1_{A_1} * \mu_{A_2}\|_{L^p}\|\mu_{A_3}\|_{L^q}$$
$$\leqslant \theta(\alpha_1/\alpha_3)^{1/p}$$
$$(4.2) \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \leqslant \theta\alpha_3^{-1/p}$$

Since $\mathbb{E}_{z \in G}1_{A_1} * \mu_{A_2} * \mu_{A_3}(z) = \alpha_1$ we may pick z so that $1_{A_1} * \mu_{A_2} * \mu_{A_3}(z) \geqslant \alpha_1$. Choosing $p = 2 + \log\alpha_3^{-1}$ and $\theta = \alpha_1/2e$ we have $\theta\alpha_3^{-1/p} \leqslant \alpha_1/2$, and by (4.2) we conclude that $1_{A_1} * \mu_{A_2} * \mu_{A_3}(z + x) \geqslant \alpha_1/2$, where $x \in B$ is arbitrary. $\square$

We may now quickly derive Theorem 1.4, which we reproduce below with adjusted notations for convenience.

Proposition (Theorem 1.4). *Suppose that A_1, A_2, A_3 are subsets of $\mathbb{Z}/N\mathbb{Z}$ of respective densities $\alpha_1, \alpha_2, \alpha_3$ and write $\widetilde{\alpha} = \alpha_1\alpha_2\alpha_3$. Then there exist absolute constants $c > 0$ and $C > 0$ such that $A_1 + A_2 + A_3$ contains an arithmetic progression of length at least*

$$N^{c\alpha_1^2/(\log 2\widetilde{\alpha}^{-1})^4} \quad \text{if} \quad \alpha_1(\log 2\widetilde{\alpha}^{-1})^{-5/2} \geqslant C(\log N)^{-1/2}$$

such that each element of the progression has at least $\frac{1}{2}\widetilde{\alpha}N^2$ representations as a sum.

Proof. Apply Proposition 4.2 to obtain a Bohr set B and an element $z \in G$ such that $d \leqslant C\alpha_1^{-2}(\log 2\widetilde{\alpha}^{-1})^4$, $\delta \geqslant c\widetilde{\alpha}^C$ and $1_{A_1} * 1_{A_2} * 1_{A_3}(y) \geqslant \frac{1}{2}\widetilde{\alpha}$ for every $y \in z + B$. By Lemma 3.5 we may find an arithmetic progression $P \subset B$ of size

$$|P| \geqslant \exp\left(\frac{c\alpha_1^2\log N}{(\log 2\widetilde{\alpha}^{-1})^4} - C\log 2\widetilde{\alpha}^{-1}\right).$$

Restricting to $\alpha_1^2(\log 2\widetilde{\alpha}^{-1})^{-5} \geqslant C'(\log N)^{-1}$ with C' large enough we see that $z + P$ is the desired arithmetic progression. $\square$

5. Preliminaries on the density-increment strategy

The proof of Theorems 1.5 and 1.6 is based on the density-increment strategy used by Bourgain [3, 4] to obtain good bounds in Roth's theorem [16] and later considerably expanded by Sanders in [20, 21]. The base of this theory is best presented in [22], while the more advanced techniques specific to Roth's theorem may be found in [20, 21]. We also use a recent refinement of those by Bloom [1]. In this section we collect the main facts that we need from these references.

We first need a special case of Lemmas 4.6 and 6.3 of [21], which together constitute a local version of Chang's spectral lemma [5, Lemmas 3.1 and 3.4].

Lemma 5.1 (Local spectrum annihilation). *Let $\varepsilon \in (0, 1]$ be a parameter. Let B be a regular Bohr set and suppose that $X \subset B$ has relative density τ. Then there exists a regular Bohr set $B' \leqslant B$ with*

$$d' \leqslant d + C\varepsilon^{-2} \log 2\tau^{-1} \quad and \quad \delta' \geqslant c\delta/(d^2\varepsilon^{-2} \log 2\tau^{-1})$$

such that $|1 - \gamma(x)| \leqslant \frac{1}{2}$ for every $\gamma \in \mathrm{Spec}_\varepsilon(\mu_X)$ and $x \in B'$.

Proof. Write $B = B(\Gamma, \delta)$ and let $\Delta = \mathrm{Spec}_\varepsilon(\mu_X)$. By Lemma 4.6 of [21], Δ has $(1, \mu_B)$-relative entropy $k \ll \varepsilon^{-2} \log 2\tau^{-1}$ (see [21] for the definition of this concept); note in passing that, by the definition of entropy, $k \geqslant 1$. Applying Lemma 6.3 of [21] to Δ with $\eta = 1$ we may further find a set Λ of size at most k such that, for every $\nu \in (0, 1), \rho \leqslant c/(dk)$ and $\gamma \in \Delta$,

$$|1 - \gamma(x)| \ll k\nu + \rho d^2(k + 1) \quad \text{uniformly in} \quad x \in B(\Gamma \cup \Lambda, \min(\rho\delta, 2\nu)).$$

Choosing $\rho = c/(d^2k)$ and $\nu = c/k$ with c small enough we see that $|1 - \gamma(x)| \leqslant \frac{1}{2}$ for $x \in B(\Gamma \cup \Lambda, c\delta/d^2k) =: \widetilde{B}$, and we are done upon choosing $B' = \widetilde{B}_\kappa$ with $\kappa \in [1/2, 1)$ chosen via Lemma 3.7 such that $\widetilde{B}$ is regular. $\qquad\square$

Note that as in [18] we need to keep track of the radius of the Bohr set rather than its size, since we are looking for arithmetic progressions such as given by Lemma 3.5. The following is Lemma 3.8 of [20] where we used the Bohr set given by Lemma 5.1 in the proof instead. This lemma forms the backbone of the density-increment strategy.

Lemma 5.2 (L^2 density-increment). *Let $\nu, \eta, \rho \in (0, 1]$ be parameters. Let B and $\dot{B} \leqslant B_\rho$ be regular Bohr sets. Suppose that $A \subset B$ has relative density α and $X \subset \dot{B}$*

has relative density τ. Write $f_A = 1_A - \alpha 1_B$, and suppose that $\rho \leqslant c\nu\alpha/d$ and

$$\sum_{\gamma \in \mathrm{Spec}_\eta(\mu_X)} |\widehat{f_A}(\gamma)|^2 \geqslant \nu\alpha^2 m_G(B).$$

Then there exists a regular Bohr set $\breve{B} \leqslant \dot{B}$ such that $\|1_A * \mu_{\breve{B}}\|_\infty \geqslant (1 + c\nu)\alpha$,

$$\breve{d} \leqslant \dot{d} + C\eta^{-2}\log 2\tau^{-1} \quad and \quad \breve{\delta} \geqslant c\dot{\delta}/(\dot{d}^2\eta^{-2}\log 2\tau^{-1}).$$

The slightly different shape of the density-increment lemma above affects in a minor way the statement of two results we introduce next. The first is the Katz-Koester transform developed by Sanders [20]; the following is Proposition 4.1 from there.

Lemma 5.3 (Katz-Koester transform). *Let $\rho, \rho' \in (0, 1)$ be parameters. Let B be a regular Bohr set, assume that $B' = B_\rho$ is regular and let $B'' = B'_{\rho'}$. Suppose that $A \subset B$ has relative density α and $A' \subset B'$ has relative density α'. Assume that $\rho \leqslant c\alpha/d$ and $\rho' \leqslant c\alpha'/d$. Then either*

(i) *there exists a regular Bohr set $\breve{B} \leqslant B'$ such that $\|1_A * \mu_{\breve{B}}\|_\infty \geqslant (1 + c)\alpha$,*

$$\breve{d} \leqslant d + C\alpha^{-1}\log 2\alpha'^{-1} \quad and \quad \breve{\delta} \geqslant c\rho(\alpha\alpha'/d)^C\delta,$$

(ii) *or there exist $L \subset B$ with relative density λ and $S \subset B''$ with relative density σ, such that $\lambda \gg 1$, $\sigma \geqslant e^{-C\alpha^{-1}\log 2\alpha'^{-1}}$ and*

$$1_L * 1_S \leqslant C\alpha^{-1} 1_A * 1_{A'}.$$

A second result we import is a generalization of the above for three of more sets due to Bloom [1]; the following is a direct consequence of the case $k = 2$ of Theorem 6.1 from there.

Lemma 5.4 (Katz-Koester transform for three sets). *Let $\rho, \rho' \in (0, 1)$ be parameters. Let B be a regular Bohr set, suppose that $B' = B_\rho$ is regular and let $B'' = B'_{\rho'}$. Suppose that $A \subset B$ has relative density α and $A'_1, A'_2 \subset B'$ have relative densities α'_1, α'_2, and write $\gamma = \alpha\alpha'_1\alpha'_2$. Assume that $\rho \leqslant c\alpha/d$ and $\rho' \leqslant c\gamma/d$. Then either*

(i) *there exists a regular Bohr set $\breve{B} \leqslant B'$ such that $\|1_A * \mu_{\breve{B}}\|_\infty \geqslant (1 + c)\alpha$,*

$$\breve{d} \leqslant d + C\alpha^{-1/2}\log 2\gamma^{-1} \quad and \quad \breve{\delta} \geqslant c\rho(\gamma/d)^C\delta,$$

(ii) *or there exist $L \subset B$ with relative density λ and $S_1, S_2 \subset B''$ with relative densities σ_1, σ_2 such that $\lambda \gg 1$, $\sigma_i \geqslant e^{-C\alpha^{-1/2}\log 2\gamma^{-1}}$, and*

$$1_L * 1_{S_1} * 1_{S_2} \leqslant C\alpha^{-2} 1_A * 1_{A'_1} * 1_{A'_2}.$$

Finally, we are going to make extensive use of the Croot-Sisask lemma [8], which says that two-fold convolutions possess large sets of almost-periods. This technique is particularly suited to prove asymmetric results such as Theorems 1.5 and 1.6. The slightly different version we quote is Lemma 3.3 of [22] due to Sanders.

Lemma 5.5 (Croot-Sisask lemma). *Let $p \geqslant 2$ and $\varepsilon \in (0,1)$ be a pair of parameters. Let $f : G \to \mathbb{C}$ and $L \geqslant 1$ and assume that S and T are subsets of G such that $|S + T| \leqslant L|S|$. Then there exist $t \in T$ and a set $X \subset T$ of size $|X| \geqslant (2L)^{-Cp/\varepsilon^2}|T|$ such that*

$$\|f * \mu_S - \tau_y f * \mu_S\|_{L^p} \leqslant \varepsilon \|f\|_{L^p} \qquad (y \in X - t).$$

This has the following familiar consequence, often used implicitly throughout the literature.

Lemma 5.6 (L^p-smoothing of convolutions). *Let $p \geqslant 2$, $\ell \geqslant 1$ and $\theta \in (0,1)$ be parameters. Let $f : G \to \mathbb{C}$ and $L \geqslant 1$ and suppose that S and T are subsets of G such that $|S + T| \leqslant L|S|$. Then there exists a set $X \subset T$ of size $|X| \geqslant (2L)^{-Cp\ell^2/\theta^2}|T|$ such that*

$$\|f * \mu_S - f * \mu_S * \lambda_X^{(\ell)}\|_{L^p} \leqslant \theta \|f\|_{L^p}$$

where $\lambda_X = \mu_X * \mu_{-X}$.

Proof. Apply Lemma 5.5 with parameter $\varepsilon = \theta/(2\ell)$. By the triangle inequality and the translation-invariance of L^p-norms we have, for every $x_1, \ldots, x_\ell, x'_1, \ldots, x'_\ell \in X$:

$$\|f * \mu_S - \tau_{x_1 - x'_1 + \cdots + x_\ell - x'_\ell} f * \mu_S\|_{L^p} \leqslant \theta \|f\|_{L^p}.$$

By averaging over the numerous x_i, x'_j and the triangle inequality we recover the result. $\square$

6. Proof of Theorems 1.5 and 1.6

We are now ready to start with the proof of our main estimates. In this section we introduce a new piece of notation to make computations more bearable: to every Bohr set B we associate the **density parameter** $b = m_G(B)$. We start with an easy consequence of regularity which gives us some control on the size of scaled-down sets.

Lemma 6.1 (Scaling lemma). *Let $\rho \in (0,1)$ be a parameter. Let B be a regular Bohr set and $B' \subset B_\rho$. Suppose that $A \subset B$ has relative density α and $\rho \leqslant c/d$, then*

$$\|1_A * \mu_{B'}\|_\infty \geqslant (1 - O(\tfrac{\rho d}{\alpha}))\alpha.$$

Proof. We have, by Lemma 3.8,

$$\mathbb{E}_{x \in B} 1_A * \mu_{B'}(x) = \langle 1_A * \mu_{B'}, \mu_B \rangle_{L^2}$$

$$= \langle 1_A, \mu_B * \mu_{B'} \rangle_{L^2}$$

$$= \langle 1_A, \mu_B \rangle_{L^2} + O\big(\|\mu_B - \mu_B * \mu_{B'}\|_{L^1} \|1_A\|_\infty \big)$$

$$= \alpha + O(\rho d).$$

Bounding the left-hand side in $\| \cdot \|_\infty$ norm concludes the proof. $\qquad \square$

Our iterative argument intially follows that developed by Sanders in [18], with slight modifications to accomodate upper level sets. We recall its principle here. At each step, one fixes a small Bohr set B' and finds a translate A_3' of A_3 with relative density in B' of same order as that of A_3 in B. Then either B' is contained in the upper level set $\{1_{A_1} * 1_{A_2} * 1_{A_3'} > K\}$, or it has non-empty intersection $\mathcal{U}$ with the lower level set $\{1_{A_1} * 1_{A_2} * 1_{A_3'} \leqslant K\}$. The scalar product $\langle 1_{A_1} * 1_{A_2} * 1_{A_3'}, 1_{\mathcal{U}} \rangle_{L^2}$ is then unusually small for a good choice of K. The usual density-increment strategy then allows one to find a smaller Bohr set on which either A_1 or A_2 has increased density. Since the density is bounded by 1 we may iterate this process only a finite number of times, after which we have found a translate of a Bohr set in a certain upper level set.

At this point however we take advantage of two techniques from [20], which we apply in a similar fashion. The first is the Katz-Koester transform which in this situation roughly redistributes the mass of the sets A_1 and A_3' on two new sets L and S where L is thick and S is not too small, without affecting the size of the convolution $1_{A_1} * 1_{A_3'}$ excessively. The second is the Croot-Sisask lemma which allows one to smooth the convolution $1_L * 1_S$ by a factor $\lambda_X^{(\ell)}$. At last the density-increment strategy makes it possible to exploit the smallness of the new scalar product $\langle 1_L * 1_S * 1_{A_2} * \lambda_X^{(\ell)}, 1_{\mathcal{U}} \rangle$ to obtain a density increment on A_2.

Our main iterative lemma is then the following. On a first reading the reader may wish to take $\omega = 0$ below for simplicity, which suffices to obtain Theorem 1.5 without a counting lemma.

Proposition 6.2 (Main iterative lemma). *Let $\rho, \omega \in (0, 1)$ be parameters. Let B be a regular Bohr set and suppose that $B' = B_\rho$ is regular. Suppose that $A_1, A_2, A_3 \subset B$ have relative densities $\alpha_1, \alpha_2, \alpha_3$ and write $\widetilde{\alpha} = \alpha_1 \alpha_2 \alpha_3$. Assume that $\rho \leqslant c\widetilde{\alpha}/d$ and $\omega \leqslant e^{-C(d+\alpha_1^{-1}) \log(2d/\rho\widetilde{\alpha})}$. Then either*

(i) *there exists a regular Bohr set $\check{B} \leqslant B$ such that, for some $i \in \{1, 2\}$,*

$$\|1_{A_i} * \mu_{\check{B}}\|_\infty \geqslant (1+c)\alpha_i,$$

$$\check{d} \leqslant d + C\alpha_1^{-1}(\log 2\widetilde{\alpha}^{-1})^4,$$

$$\check{\delta} \geqslant c\rho(\widetilde{\alpha}/d)^C\delta,$$

(ii) *or there exists $x \in G$ such that $B' \subset \{\, y \,:\, 1_{A_1} * 1_{A_2} * 1_{A_3}(x+y) > \omega b^2 \,\}$.*

Proof. By Lemma 6.1 we may find $x \in G$ such that $A_3' = (A_3 - x) \cap B'$ has relative density in B' equal to $\alpha_3' = 1_{A_3} * \mu_{B'}(x) \gg \alpha_3$. Now define

$$\mathcal{U} = \{\, y \,:\, 1_{A_1} * 1_{A_2} * 1_{A_3}(x+y) \leqslant \omega b^2 \,\} \cap B',$$

we may assume that $\mathcal{U}$ is non-empty since else we are in the second case of the proposition. Note that from the inclusion $A_3' \subset A_3 - x$ and the definition of $\mathcal{U}$ we have

$$\langle 1_{A_1} * 1_{A_2} * 1_{A_3'}, \mu_{\mathcal{U}} \rangle_{L^2} \leqslant \langle 1_{A_1} * 1_{A_2} * 1_{A_3-x}, \mu_{\mathcal{U}} \rangle_{L^2}$$

$$= \langle 1_{A_1} * 1_{A_2} * 1_{A_3}, \mu_{x+\mathcal{U}} \rangle_{L^2}$$

(6.1) $$\leqslant \omega b^2$$

where $\mu_{\mathcal{U}}$ is well-defined since $\mathcal{U} \neq \varnothing$. From hereon the proof divides into three steps.

Applying the Katz-Koester transform. Let $\rho' = c\kappa\alpha_3/d$ and $B'' = B'_{\rho'}$, where $\kappa \in [1/2, 1)$ is chosen via Lemma 3.7 so that B'' is regular. Applying Lemma 5.3 to $A = A_1$ and $A' = A_3'$ with parameters ρ and ρ' then results in one of two cases. In case (i) of that lemma we obtain a regular Bohr set $\check{B} \leqslant B'$ such that $\|1_{A_1} * \mu_{\check{B}}\|_\infty \geqslant (1+c)\alpha_1$,

$$\check{d} \leqslant d + C\alpha_1^{-1}\log 2\alpha_3^{-1} \quad \text{and} \quad \check{\delta} \geqslant c\rho(\alpha_1\alpha_3/d)^C\delta,$$

which is enough to conclude. In case (ii), we may find $L \subset B$ with relative density λ and $S \subset B''$ with relative density σ such that

(6.2) $$\lambda \gg 1 \quad \text{and} \quad \sigma \geqslant e^{-C\alpha_1^{-1}\log 2\alpha_3^{-1}},$$

(6.3) $$1_L * 1_S \ll \alpha_1^{-1} 1_{A_1} * 1_{A_3'}.$$

By (6.3) we then have

$$\langle 1_L * \mu_S, 1_{-A_2} * \mu_{\mathcal{U}} \rangle_{L^2} = (\sigma b'')^{-1} \langle 1_L * 1_S, 1_{-A_2} * \mu_{\mathcal{U}} \rangle_{L^2}$$

$$\ll (\alpha_1 \sigma b'')^{-1} \langle 1_{A_1} * 1_{A_3'}, 1_{-A_2} * \mu_{\mathcal{U}} \rangle_{L^2}$$

$$= (\alpha_1 \sigma b'')^{-1} \langle 1_{A_1} * 1_{A_2} * 1_{A_3'}, \mu_{\mathcal{U}} \rangle_{L^2}.$$

By (6.1) we have further

$$\langle 1_L * \mu_S, 1_{-A_2} * \mu_{\mathcal{U}} \rangle_{L^2} \ll (\alpha_1 \sigma b'')^{-1} \omega b^2$$
$$= (\lambda \alpha_1 \alpha_2 \sigma)^{-1}(b/b'') \omega \cdot \lambda \alpha_2 b.$$

Recalling (6.2) and applying Lemma 3.3 we have therefore

$$\langle 1_L * \mu_S, 1_{-A_2} * \mu_{\mathcal{U}} \rangle_{L^2} \leqslant e^{C(d+\alpha_1^{-1})\log(2d/\rho\widetilde{\alpha})} \omega \cdot \lambda \alpha_2 b.$$

Assuming $\omega \leqslant e^{-C'(d+\alpha_1^{-1})\log(2d/\rho\widetilde{\alpha})}$ with C' large enough we eventually obtain

$$(6.4) \qquad \langle 1_L * \mu_S, 1_{-A_2} * \mu_{\mathcal{U}} \rangle_{L^2} \leqslant \tfrac{1}{4}\lambda \alpha_2 b.$$

Applying the Croot-Sisask lemma. Let $\rho'' = c\kappa'/d$ and $B''' = B''_{\rho''}$, where $\kappa' \in [1/2, 1)$ is chosen via Lemma 3.7 so that B''' is regular, and with c small enough so that, by regularity of B'' and Definition 3.6,

$$|S + B'''| \leqslant |B'' + B'''| \leqslant |B''_{1+\rho''}| \leqslant 2|B''| = (2/\sigma)|S|.$$

Applying Lemma 5.6 to $f = 1_L$ and $T = B'''$ with parameters p, ℓ, θ to be determined later, we obtain a set $X \subset B'''$ of relative density τ with

$$(6.5) \qquad \tau \geqslant \exp\big(-C(p\ell^2/\theta^2)\log 2\sigma^{-1}\big)$$

such that

$$\|1_L * \mu_S - 1_L * \mu_S * \lambda_X^{(\ell)}\|_{L^p} \leqslant \theta \|1_L\|_{L^p}.$$

By Hölder's and Young's inequalities we have therefore

$$|\langle 1_L * \mu_S, 1_{-A_2} * \mu_{\mathcal{U}} \rangle_{L^2} - \langle 1_L * \mu_S * \lambda_X^{(\ell)}, 1_{-A_2} * \mu_{\mathcal{U}} \rangle_{L^2}|$$
$$\leqslant \|1_L * \mu_S - 1_L * \mu_S * \lambda_X^{(\ell)}\|_{L^p}\|1_{-A_2} * \mu_{\mathcal{U}}\|_{L^q}$$
$$\leqslant \theta \|1_L\|_{L^p}\|1_{-A_2}\|_{L^q}$$
$$= \theta \lambda^{1/p}\alpha_2^{1-1/p}b$$

Choosing $p = 2 + \log \alpha_2^{-1}$ and $\theta = \lambda^{1-1/p}/4e \asymp 1$ this is less than $\tfrac{1}{4}\lambda \alpha_2 b$, which combined with (6.4) shows that

$$(6.6) \qquad |\langle 1_L * \mu_S * \lambda_X^{(\ell)}, 1_{-A_2} * \mu_{\mathcal{U}} \rangle_{L^2}| \leqslant \tfrac{1}{2}\lambda \alpha_2 b.$$

Obtaining an L^2 density-increment. Since $\mathcal{U}, S, X$ are contained in B', the function $\mu_{\mathcal{U}} * \mu_{-S} * \lambda_X^{(\ell)}$ has support in $(2\ell+2)B' \subset B_{(2\ell+2)\rho}$ and we have, by Lemma 3.8,

$$\langle 1_L * \mu_S * \lambda_X^{(\ell)}, 1_B * \mu_{\mathcal{U}} \rangle_{L^2} = \langle 1_L, 1_B * \mu_{\mathcal{U}} * \mu_{-S} * \lambda_X^{(\ell)} \rangle_{L^2}$$

$$= \langle 1_L, 1_B \rangle_{L^2} + O\big(\|1_B - 1_B * \mu_{\mathcal{U}} * \mu_{-S} * \lambda_X^{(\ell)}\|_{L^1} \|1_L\|_\infty \big)$$

$$= \lambda b + O(\ell \rho d b)$$

$$(6.7) \hspace{4cm} \geqslant \tfrac{3}{4}\lambda b$$

provided that $\rho \leqslant c/(\ell d)$, which will turn out to be the case. Forming the balanced function $f_{-A_2} = 1_{-A_2} - \alpha_2 1_B$, we deduce from (6.6) and (6.7) that

$$|\langle 1_L * \mu_S * \lambda_X^{(\ell)}, f_{-A_2} * \mu_{\mathcal{U}} \rangle_{L^2}| \geqslant \tfrac{1}{4}\lambda \alpha_2 b.$$

By Parseval's formula and the inequality $\|\widehat{f}\|_\infty \leqslant \|f\|_{L^1}$ we have therefore

$$\tfrac{1}{4}\lambda \alpha_2 b \leqslant \big| \langle \widehat{1_L} \cdot \widehat{\mu_S} \cdot \widehat{\mu_X}^\ell \cdot \widehat{\mu_{-X}}^\ell, \widehat{f_{-A_2}} \cdot \widehat{\mu_{\mathcal{U}}} \rangle_{\ell^2} \big|$$

$$\leqslant \|\widehat{\mu_S}\|_\infty \|\widehat{\mu_{\mathcal{U}}}\|_\infty \|\widehat{1_L} \cdot \widehat{f_{A_2}} \cdot \widehat{\mu_X}^{2\ell}\|_{\ell^1}$$

$$\leqslant \|\widehat{1_L} \cdot \widehat{f_{A_2}} \cdot \widehat{\mu_X}^{2\ell}\|_{\ell^1}.$$

By Cauchy-Schwartz and Parseval's identity we then have

$$\tfrac{1}{4}\lambda \alpha_2 b \leqslant \|\widehat{1_L}\|_{\ell^2} \|\widehat{f_{A_2}} \cdot \widehat{\mu_X}^{2\ell}\|_{\ell^2} = (\lambda b)^{1/2} \|\widehat{f_{A_2}} \cdot \widehat{\mu_X}^{2\ell}\|_{\ell^2}.$$

It follows that, for some constant c,

$$(6.8) \hspace{3cm} \sum_\gamma |\widehat{f_{A_2}}(\gamma)|^2 |\widehat{\mu_X}(\gamma)|^{4\ell} \geqslant \tfrac{1}{16}\lambda \alpha_2^2 b \geqslant c\alpha_2^2 b.$$

By Parseval's identity and choosing $\ell = C \log 2\alpha_2^{-1}$ with C large enough we have

$$\sum_{\gamma : |\widehat{\mu_X}(\gamma)| \leqslant 1/2} |\widehat{f_{A_2}}(\gamma)|^2 |\widehat{\mu_X}(\gamma)|^{4\ell} \leqslant 2^{-4\ell} \|f_{A_2}\|_{L^2}^2$$

$$\leqslant 2^{2-4\ell} \alpha_2 b$$

$$\leqslant \tfrac{1}{2} c\alpha_2^2 b.$$

By (6.8) and the bound $\|\widehat{\mu_X}\|_\infty \leqslant 1$ we have therefore

$$\sum_{\gamma \in \mathrm{Spec}_{1/2}(\mu_X)} |\widehat{f_{A_2}}(\gamma)|^2 \gg \alpha_2^2 b.$$

The parameters we have chosen have size $p \asymp \log 2\alpha_2^{-1}$, $\ell \asymp \log 2\alpha_2^{-1}$, and $\theta \asymp 1$, and therefore by (6.5) and (6.2) we have

$$\tau \geqslant \exp\left(-C\alpha_1^{-1}(\log 2\widetilde{\alpha}^{-1})^4\right).$$

Since $\rho' \asymp \alpha_3/d$ and $\rho'' \asymp 1/d$ we also have $\delta''' = c\rho(\alpha_3/d^2)\delta$. Applying Lemma 5.2 with $A = A_2$ and for $\eta = 1/2$ and some $\nu \asymp 1$ we therefore obtain a regular Bohr set $\breve{B} \leqslant B'''$ such that $\|1_{A_2} * \mu_{\breve{B}}\|_\infty \geqslant (1+c)\alpha_2$ and

$$\breve{d} \leqslant d + C\alpha_1^{-1}(\log 2\widetilde{\alpha}^{-1})^4 \quad \text{and} \quad \breve{\delta} \geqslant c\rho(\widetilde{\alpha}/d)^4\delta,$$

which again is enough to conclude. $\qquad\square$

We are now in a position to prove the following result, which gives slightly more structure than Theorem 1.5 in the form of a translate of a large Bohr set. Theorem 1.5 will then follow quickly from this proposition and Lemma 3.5.

Proposition 6.3. *Suppose that A_1, A_2, A_3 are subsets of $\mathbb{Z}/N\mathbb{Z}$ of respective densities $\alpha_1, \alpha_2, \alpha_3$ and write $\widetilde{\alpha} = \alpha_1\alpha_2\alpha_3$. Then there exist $z \in G$ and a Bohr set B with*

$$d \leqslant C\alpha_1^{-1}(\log 2\widetilde{\alpha}^{-1})^5,$$
$$\delta \geqslant \exp\left(-C(\log 2\widetilde{\alpha}^{-1})^2\right),$$

such that, for every $y \in z + B$,

$$1_{A_1} * 1_{A_2} * 1_{A_3}(y) > \exp\left(-C\alpha_1^{-1}(\log 2\widetilde{\alpha}^{-1})^7\right).$$

Proof. The proof proceeds by iteration of Proposition 6.2. We construct iteratively a sequence of regular Bohr sets $B^{(i)}$ and sequences of sets $A_1^{(i)}, A_2^{(i)}, A_3^{(i)} \subset B^{(i)}$ of relative densities $\alpha_1^{(i)}, \alpha_2^{(i)}, \alpha_3^{(i)}$. We initiate the iteration with $B^{(1)} = B(\{0\}, 2) = \mathbb{Z}/N\mathbb{Z}$, which is regular, and with $(A_1^{(1)}, A_2^{(1)}, A_3^{(1)}) = (A_1, A_2, A_3)$. We denote by δ_i, d_i, b_i respectively the radius, dimension and density in G of $B^{(i)}$, and we write $\widetilde{\alpha}^{(i)} = \alpha_1^{(i)}\alpha_2^{(i)}\alpha_3^{(i)}$.

At each step i we apply Proposition 6.2 to the sets $A_1^{(i)}, A_2^{(i)}, A_3^{(i)}$ with parameters ω_i and ρ_i to be determined later. In case (i) of that proposition we define $B^{(i+1)} = \breve{B}^{(i)}$, while in case (ii) we stop the iteration. Whenever $B^{(i+1)}$ is defined we pick $(x_{j,i})_{1\leqslant j\leqslant 3}$ so that, for every j, $A_j^{(i+1)} := (A_j^{(i)} - x_{j,i}) \cap B^{(i+1)}$ has relative density in $B^{(i+1)}$ equal to

$$\alpha_j^{(i+1)} = 1_{A_j^{(i)}} * \mu_{B^{(i+1)}}(x_{j,i}) = \|1_{A_j^{(i)}} * \mu_{B^{(i+1)}}\|_\infty.$$

We now assume that $B^{(i)}$ is defined for $1 \leqslant i \leqslant n$. Let $i < n$, our application of Proposition 6.2 then shows that there exists $j_i \in \{1, 2\}$ such that $\alpha_{j_i}^{(i+1)} \geqslant (1+c)\alpha_{j_i}^{(i)}$. Choose now $\rho_i = c'\kappa_i\widetilde{\alpha}^{(i)}/(2i^2 d_i)$, where $\kappa_i \in [1/2, 1)$ is picked via Lemma 3.7 so that

$B_{\rho_i}^{(i)}$ is regular, and with c' small enough so that, by Lemma 6.1,

$$(6.9) \qquad \alpha_j^{(i+1)} \geqslant \left(1 - O(\rho_i d_i / \alpha_j^{(i)})\right) \alpha_j^{(i)} \geqslant \left(1 - \tfrac{c}{2i^2}\right) \alpha_j^{(i)}$$

for every $1 \leqslant j \leqslant 3$. This implies that

$$\alpha_1^{(i+1)} \alpha_2^{(i+1)} \geqslant (1 - c/2)(1 + c) \alpha_1^{(i)} \alpha_2^{(i)} \geqslant (1 + c/4) \alpha_1^{(i)} \alpha_2^{(i)},$$

and as a consequence the iteration proceeds for at most $n = O(\log 2\widetilde{\alpha}^{-1})$ steps. Iterating (6.9) we also obtain

$$\alpha_j^{(i)} \geqslant e^{-O(\sum_{i=1}^{\infty} i^{-2})} \alpha_j \gg \alpha_j$$

uniformly in $1 \leqslant j \leqslant 3$ and $1 \leqslant i \leqslant n$. The dimension bound from Proposition 6.2 then becomes

$$d_{i+1} \leqslant d_i + (C/\alpha_1^{(i)}) \log^4(2/\widetilde{\alpha}^{(i)}) \leqslant d_i + O\left(\alpha_1^{-1} \log^4(2/\widetilde{\alpha})\right)$$

for $i < n$ and therefore $d_i \ll i\alpha_1^{-1}(\log 2\widetilde{\alpha}^{-1})^4 \ll \alpha_1^{-1}(\log 2\widetilde{\alpha}^{-1})^5$ uniformly in $1 \leqslant i \leqslant n$. The radius bound from Proposition 6.2 is then

$$\delta_{i+1} \geqslant (\widetilde{\alpha}^{(i)}/2id_i)^{O(1)} \delta_i \geqslant (\widetilde{\alpha}/2)^{O(1)} \delta_i$$

for $i < n$ whence $\delta_i \geqslant (\widetilde{\alpha}/2)^{O(i)} \geqslant e^{-O((\log 2\widetilde{\alpha}^{-1})^2)}$ uniformly in $1 \leqslant i \leqslant n$.

Finally we choose $\omega_i = \omega$ independent of i so as to satisfy the condition

$$\omega \leqslant \exp\left(-C(d_i + (\alpha_1^{(i)})^{-1}) \log(2d_i/\rho_i\widetilde{\alpha}^{(i)})\right)$$

from Proposition 6.2 for every $1 \leqslant i \leqslant n$. From the previous dimension and radius bounds we see that it is enough to take $\omega = e^{-C'\alpha_1^{-1}(\log 2\widetilde{\alpha}^{-1})^6}$, with C' large enough. For that choice we deduce from Lemma 3.4 and the bounds on d_i and δ_i that $\omega b_i^2 \geqslant e^{-O(\alpha_1^{-1}(\log 2\widetilde{\alpha}^{-1})^7)}$ uniformly in $1 \leqslant i \leqslant n$. When we are in case (ii) of Proposition 6.2 we therefore find that $B_{\rho_n}^{(n)}$ is contained in a translate of

$$\left\{ y : 1_{A_1^{(n)}} * 1_{A_2^{(n)}} * 1_{A_3^{(n)}}(y) \geqslant \exp\left(-C\alpha_1^{-1}(\log 2\widetilde{\alpha}^{-1})^7\right) \right\}.$$

Since $\rho_n \geqslant (\widetilde{\alpha}/2)^{O(1)}$ and the $A_j^{(n)}$ are, by construction, contained in translates of the A_j, this concludes the proof. $\qquad \square$

Proof of Theorem 1.5. Applying Proposition 6.3 with $(A_1, A_2, A_3) = (A, B, C)$ and using Lemma 3.5 we may find an arithmetic progression P such that

$$|P| \geqslant \exp\left(\frac{c\alpha(\log N)}{(\log(2/\alpha\beta\gamma))^5} - C(\log(2/\alpha\beta\gamma))^2\right)$$

and an element $z \in G$ such that $1_{A_1} * 1_{A_2} * 1_{A_3}(y) \geqslant e^{-C\alpha^{-1} \log^7(2/\alpha\beta\gamma)}$ for all $y \in z + P$. Restricting to $\alpha(\log \frac{2}{\alpha\beta\gamma})^{-7} \geqslant C'(\log N)^{-1}$ with C' large enough we see that $z + P$ is the desired arithmetic progression. $\qquad \square$

We now turn to the slightly more difficult proof of Theorem 1.6. The main strategy is the same and we again start with a small scalar product $\langle 1_{A_1} * 1_{A_3'} * 1_{-\mathcal{U}}, 1_{-A_2} \rangle$ where $\mathcal{U}$ is a certain lower level set. However we now fully exploit the set $\mathcal{U}$ in applying the generalized Katz-Koester transform from [1] to the three sets $A_1, A_3', -\mathcal{U}$. This redistributes the mass more efficiently and accounts for the improved dependency on densities. The rest of the proof runs similarly with applications of the Croot-Sisask lemma and the density-increment strategy.

This however requires us to assume that $\mathcal{U} = \{1_{A_1} * 1_{A_2} * 1_{A_3'} \leqslant K\}$ is dense enough inside a Bohr set B'. We are then in a situation already encountered in [18] where at each step of the iteration it either happens that $\mathcal{U}$ has low density and that the upper level set $\mathcal{U}^c = \{1_{A_1} * 1_{A_2} * 1_{A_3'} > K\}$ is thick inside B'; or that a density increment can be obtained. The following lemma makes this precise and the reader may again let $\omega = 0$ there to obtain Theorem 1.6 without a counting lemma.

Proposition 6.4 (Main iterative lemma). *Let $\rho, v, \omega \in (0,1)$ be parameters. Let B be a regular Bohr set and assume that $B' = B_\rho$ is regular. Suppose that $A_1, A_2, A_3 \subset B$ have relative densities $\alpha_1, \alpha_2, \alpha_3$ and write $\widetilde{\alpha} = \alpha_1 \alpha_2 \alpha_3$. Assume that $\rho \leqslant c\widetilde{\alpha}/d$ and $w \leqslant e^{-C(d+\alpha_1^{-1/2})\log(2d/\rho v \widetilde{\alpha})}$. Then either*

(i) *there exists a regular Bohr set $\breve{B} \leqslant B$ and $i \in \{1,2\}$ such that*

$$\|1_{A_i} * \mu_{\breve{B}}\|_\infty \geqslant (1+c)\alpha_i,$$
$$\breve{d} \leqslant d + C\alpha_1^{-1/2}(\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})^4,$$
$$\breve{\delta} \geqslant c\rho(v\widetilde{\alpha}/d)^C \delta,$$

(ii) *or there exists $x \in G$ such that $\{y : 1_{A_1} * 1_{A_2} * 1_{A_3}(x + y) > \omega b^2\} \cap B'$ has relative density at least $1 - v$ in B'.*

Proof. The proof is in many aspects similar to that of Proposition 6.2 and therefore we are more brief in computations. By Lemma 6.1 we may find $x \in G$ such that $A_3' = (A_3 - x) \cap B'$ has relative density $\alpha_3' = 1_{A_3} * \mu_{B'}(x) \gg \alpha_3$ in B'. Let

$$\mathcal{U} = \{y : 1_{A_1} * 1_{A_2} * 1_{A_3}(x + y) \leqslant \omega b^2\} \cap B'$$

have density u in B'; we may assume that $u \geqslant v$ since else we are in the second case of the proposition. Note that by the definitions of A'_3 and $\mathcal{U}$ we have

$$(6.10) \qquad \langle 1_{A_1} * 1_{A_2} * 1_{A'_3}, 1_{\mathcal{U}} \rangle_{L^2} \leqslant \omega b^2 \cdot ub' \leqslant \omega b^2 b'.$$

From there the proof again divides into three steps.

Applying the Katz-Koester transform. Choose $\rho' = cv\widetilde{\alpha}/d$ with the help of Lemma 3.7 so that $B'' := B'_{\rho'}$ is regular. Applying Lemma 5.4 with $(A, A'_1, A'_2) = (A_1, -\mathcal{U}, A'_3)$ then results into one of two cases. In case (i) of that lemma we obtain a regular Bohr set $\check{B} \leqslant B'$ such that $\|1_{A_1} * \mu_{\check{B}}\|_\infty \geqslant (1+c)\alpha_1$,

$$\check{d} \leqslant d + C\alpha_1^{-1/2} \log(2/v\widetilde{\alpha}) \quad \text{and} \quad \check{\delta} \geqslant c\rho(v\widetilde{\alpha}/d)^C \delta,$$

which is enough to conclude via the crude bound $\log(2/v\widetilde{\alpha}) \ll (\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})$. In case (ii), we may find $L \subset B$ of relative density λ and $S_1, S_2 \subset B''$ of relative densities σ_1, σ_2 such that

$$(6.11) \qquad \lambda \gg 1, \quad \sigma_1, \sigma_2 \geqslant e^{-C\alpha_1^{-1/2} \log(2/v\widetilde{\alpha})},$$

$$(6.12) \qquad 1_L * 1_{S_1} * 1_{S_2} \ll \alpha_1^{-2} 1_{A_1} * 1_{-\mathcal{U}} * 1_{A'_3}.$$

In that case write $I = \langle 1_L * \mu_{S_1} * \mu_{S_2}, 1_{-A_2} \rangle_{L^2}$ for convenience. By (6.12) we then have

$$I \ll (\alpha_1^2 \sigma_1 \sigma_2)^{-1}(b'')^{-2} \langle 1_{A_1} * 1_{-\mathcal{U}} * 1_{A'_3}, 1_{-A_2} \rangle_{L^2}$$
$$= (\alpha_1^2 \sigma_1 \sigma_2)^{-1}(b'')^{-2} \langle 1_{A_1} * 1_{A_2} * 1_{A'_3}, 1_{\mathcal{U}} \rangle_{L^2}.$$

By (6.10), (6.11) and Lemma 3.3 we have further

$$I \ll (\alpha_1^2 \sigma_1 \sigma_2)^{-1}(b'')^{-2} \omega b^2 b'$$
$$= (\lambda \alpha_1^2 \alpha_2 \sigma_1 \sigma_2)^{-1}(b/b'')(b'/b'')\omega \cdot \lambda \alpha_2 b$$
$$\leqslant e^{C(d+\alpha_1^{-1/2}) \log(2d/\rho v\widetilde{\alpha})} \omega \cdot \lambda \alpha_2 b.$$

Assuming $\omega \leqslant e^{-C'(d+\alpha_1^{-1/2}) \log(2d/\rho v\widetilde{\alpha})}$ with C' large enough we have therefore

$$(6.13) \qquad \langle 1_L * \mu_{S_1}, 1_{-A_2} * \mu_{-S_2} \rangle_{L^2} = I \leqslant \tfrac{1}{4}\lambda \alpha_2 b.$$

Applying the Croot-Sisask lemma. We let $B''' = B''_{\rho''}$ with $\rho'' = c/d$ chosen such that B''' is regular (via Lemma 3.7) and with c small enough so that, by regularity of B'', $|S_1 + B'''| \leqslant |B''_{1+\rho''}| \leqslant (2/\sigma_1)|S_1|$. Applying Lemma 5.6 with $f = 1_L$, $S = S_1$, $T = B'''$ and parameters p, ℓ, θ to be determined later, we obtain a set $X \subset B'''$ of

relative density τ with

(6.14)
$$\tau \geqslant \exp\left(-C(p\ell^2/\theta^2)\log 2\sigma_1^{-1}\right)$$

such that

$$\|1_L * \mu_{S_1} - 1_L * \mu_{S_1} * \lambda_X^{(\ell)}\|_{L^p} \leqslant \theta\|1_L\|_{L^p}.$$

Proceeding exactly as in the proof of Proposition 6.2 we then obtain from (6.13) that

(6.15)
$$|\langle 1_L * \mu_{S_1} * \mu_{S_2} * \lambda_X^{(\ell)}, 1_{-A_2}\rangle_{L^2}| \leqslant \tfrac{1}{2}\lambda\alpha_2 b$$

for the choice of parameters $p = 2 + \log\alpha_2^{-1}$ and $\theta = \lambda^{1-1/p}/4e \asymp 1$.

Obtaining an L^2 density-increment. Since the support of $\mu_{S_1} * \mu_{S_2} * \lambda_X^{(\ell)}$ is contained in $(2\ell + 2)B' \subset B_{(2\ell+2)\rho}$ we have, by Lemma 3.8,

(6.16)
$$\langle 1_L * \mu_{S_1} * \mu_{S_2} * \lambda_X^{(\ell)}, 1_B\rangle_{L^2} = \lambda b + O(\ell\rho db) \geqslant \tfrac{3}{4}\lambda b$$

provided that $\rho \leqslant c/(\ell d)$, which will turn out to be the case. Forming the balanced function $f_{-A_2} = 1_{-A_2} - \alpha_2 1_B$, we see from (6.15) and (6.16) that

$$|\langle 1_L * \mu_{S_1} * \mu_{S_2} * \lambda_X^{(\ell)}, f_{-A_2}\rangle_{L^2}| \geqslant \tfrac{1}{4}\lambda\alpha_2 b$$

A computation entirely analogous to that in the proof of Proposition 6.2 then shows that, choosing $\ell = C\log 2\alpha_2^{-1}$ with C large enough, we have

$$\sum_{\gamma\in\mathrm{Spec}_{1/2}(\mu_X)} |\widehat{f_{A_2}}(\gamma)|^2 \gg \alpha_2^2 b.$$

The parameters we have chosen have size $p \asymp \log 2\alpha_2^{-1}$, $\ell \asymp \log 2\alpha_2^{-1}$ and $\theta \asymp 1$. By (6.14), (6.11) and the bound $\log(2/v\widetilde{\alpha}) \ll (\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})$, we have therefore

$$\tau \geqslant \exp\left(-C\alpha_1^{-1/2}(\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})^4\right).$$

Since $\rho' \asymp v\widetilde{\alpha}/d$ and $\rho'' \asymp 1/d$ we also have $\delta''' = c\rho(v\widetilde{\alpha}/d^2)\delta$. Applying Lemma 5.2 to $A = A_2$ with $\eta = 1/2$ and some $\nu \asymp 1$ we obtain a regular Bohr set $\breve{B} \leqslant B'''$ such that

$$\|1_{A_2} * \mu_{\breve{B}}\|_\infty \geqslant (1 + c)\alpha_2,$$
$$\breve{d} \leqslant d + C\alpha_1^{-1/2}(\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})^4,$$
$$\breve{\delta} \geqslant c\rho(v\widetilde{\alpha}/d)^4\delta,$$

which again is enough to conclude. □

Due to the shape of Proposition 6.4 we now need to find arithmetic progressions in thick subsets of Bohr sets. This is precisely addressed by Lemma 6.7 from [18] which we now quote.

Lemma 6.5. *Let $v \in (0,1)$ be parameter and let B be a regular Bohr set. Suppose that $v^{-1} \leqslant c\delta N^{1/d}/d$ and $A \subset B$ has relative density at least $1 - v$, then A contains an arithmetic progression of length at least $4v^{-1}$.*

We now modify our iterative lemma so as to yield arithmetic progressions in upper level sets and so as to bound the number of steps in the iteration more easily.

Proposition 6.6 (Final iterative lemma)**.** *Let $\rho, v, \omega \in (0,1)$ be parameters. Let B be a regular Bohr set and assume that $B' = B_\rho$ is regular. Suppose that $A_1, A_2, A_3 \subset B$ have relative densities $\alpha_1, \alpha_2, \alpha_3$ and write $\widetilde{\alpha} = \alpha_1 \alpha_2 \alpha_3$. Assume that $\rho \leqslant c\widetilde{\alpha}/d$,*

$$(6.17) \qquad v^{-1} \leqslant c\delta' N^{1/d}/d \quad and \quad 0 \leqslant \omega \leqslant \exp\left(-C(d + \alpha_1^{-1/2})\log(2d/\rho v\widetilde{\alpha})\right).$$

Then either

(i) *there exists a regular Bohr set $\check{B} \leqslant B'$ such that*

$$\prod_{1 \leqslant j \leqslant 3} \|1_{A_j} * \mu_{\check{B}}\|_\infty \geqslant (1 + c)\widetilde{\alpha},$$

$$\check{d} \leqslant d + C\alpha_1^{-1/2}(\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})^4,$$

$$\check{\delta} \geqslant c\rho(v\widetilde{\alpha}/d)^C \delta,$$

(ii) *or the set $\{y : 1_{A_1} * 1_{A_2} * 1_{A_3}(y) > \omega b^2\}$ contains an arithmetic progression of length at least $4v^{-1}$.*

Proof. By Proposition 6.4 we may either find $x \in G$ such that

$$\mathcal{V} = \{y : 1_{A_1} * 1_{A_2} * 1_{A_3}(y + x) > \omega b^2\} \cap B'$$

has relative density at least $1 - v$ in B', in which case we may conclude by Lemma 6.5 with $A = \mathcal{V}$; or we may obtain a regular Bohr set $\check{B}$ such that $\|1_{A_i} * \mu_{\check{B}}\|_\infty \geqslant (1 + c)\alpha_i$ for some $i \in \{1, 2\}$ and with the prescribed radius and dimension bounds. Picking j, k such that $\{i, j, k\} = \{1, 2, 3\}$, Lemma 6.1 then shows that

$$\prod_{1 \leqslant \ell \leqslant 3} \|1_{A_\ell} * \mu_{\check{B}}\|_\infty \geqslant (1 + c)(1 - O(\tfrac{\rho d}{\alpha_j}))(1 - O(\tfrac{\rho d}{\alpha_k}))\widetilde{\alpha}$$

and assuming $\rho \leqslant c'\widetilde{\alpha}/d$ with c' small enough this is indeed more than $(1 + c/2)\widetilde{\alpha}$. $\qquad\square$

We are now ready for the proof of Theorem 1.6, which we quote below with adjusted notations for convenience.

Proposition (Theorem 1.6). *Let $\varepsilon \in (0, 1)$ be a parameter and suppose that A_1, A_2, A_3 are subsets of $\mathbb{Z}/N\mathbb{Z}$ of respective densities $\alpha_1, \alpha_2, \alpha_3$, and write $\widetilde{\alpha} = \alpha_1 \alpha_2 \alpha_3$. Then $A_1 + A_2 + A_3$ contains an arithmetic progression P of length at least*

$$\exp\left(c\varepsilon^{1/2}\alpha_1^{1/4}(\log N)^{1/2}(\log 2\widetilde{\alpha}^{-1})^{-7/2}\right) \quad \text{if} \quad \alpha_1(\log 2\widetilde{\alpha}^{-1})^{-14} \geqslant C(\varepsilon \log N)^{-2}$$

and such that $1_{A_1} * 1_{A_2} * 1_{A_3}(x) \geqslant N^{-\varepsilon}$ for every $x \in P$.

Proof. The proof proceeds by iteration of Proposition 6.6. We are brief since the iteration process is very similar to that of the proof of Proposition 6.3.

We construct iteratively a sequence of regular Bohr sets $B^{(i)}$ with parameters d_i, δ_i, b_i and, for every $1 \leqslant j \leqslant 3$, a sequence of sets $A_j^{(i)} \subset B^{(i)}$ of relative density $\alpha_j^{(i)}$, and we write $\widetilde{\alpha}^{(i)} = \alpha_1^{(i)}\alpha_2^{(i)}\alpha_3^{(i)}$. We initiate the iteration with $B^{(1)} = \mathbb{Z}/N\mathbb{Z}$ and $A_j^{(1)} = A_j$ for $1 \leqslant j \leqslant 3$. At each step i we apply Proposition 6.6 to the sets $A_j^{(i)}$ with parameters ρ_i, v, ω to be determined later (note that v and ω are chosen independent of i), and in case (i) we define $B^{(i+1)} = \check{B}^{(i)}$, while in case (ii) we stop the iteration. For every $1 \leqslant j \leqslant 3$ we pick $x_{i,j}$ so that $A_j^{(i+1)} := (A_j - x_{i,j}) \cap B^{(i+1)}$ has relative density $\alpha_j^{(i+1)} = \|1_{A_j^{(i)}} * \mu_{B^{(i+1)}}\|_\infty$ in $B^{(i+1)}$, whenever $B^{(i+1)}$ is defined.

By the density-increment $\widetilde{\alpha}^{(i+1)} \geqslant (1 + c)\widetilde{\alpha}^{(i)}$ from Proposition 6.6 we see that the iteration stops after at most $n = O(\log 2\widetilde{\alpha}^{-1})$ steps. We choose $\rho_i = c\widetilde{\alpha}^{(i)}/(i^2 d_i)$ such that $B_{\rho_i}^{(i)}$ is regular (via Lemma 3.7). By Lemma 6.1 we then have $\alpha_j^{(i+1)} \geqslant (1 - O(i^{-2}))\alpha_j^{(i)}$ for every i, j and therefore $\alpha_j^{(i)} \geqslant e^{-O(\sum_{i=1}^{\infty} i^{-2})}\alpha_j \gg \alpha_j$ uniformly in $1 \leqslant j \leqslant 3$ and $1 \leqslant i \leqslant n$. We then have, from the bounds of Proposition 6.6,

$$d_{i+1} \leqslant d_i + C\alpha_1^{-1/2}(\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})^4$$

for $i < n$ and therefore $d_i \leqslant C\alpha_1^{-1/2}(\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})^5$ uniformly in $1 \leqslant i \leqslant n$. Bounding crudely $\log(2/v\widetilde{\alpha}) \ll (\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})$ we also have

$$\delta_{i+1} \geqslant \exp\left(-C(\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})\right)\delta_i$$

for $i < n$ and therefore $\delta_i \geqslant \exp\left(-C(\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})^2\right)$ uniformly in $1 \leqslant i \leqslant n$.

We now choose v and ω so that (6.17) is satisfied at every step. From the previous dimension and radius bounds, we see that a sufficient condition for v is

$$\log 2v^{-1} \leqslant \frac{c\alpha_1^{1/2}\log N}{(\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})^5} - C(\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})^2.$$

We choose v defined by $\log 2v^{-1} = c'\varepsilon^{1/2}\alpha_1^{1/4}(\log N)^{1/2}(\log 2\widetilde{\alpha}^{-1})^{-7/2}$ with c' small enough so as to satisfy this; since $\log 2v^{-1} \in [\log 2, +\infty)$ this requires $\alpha_1(\log 2\widetilde{\alpha}^{-1})^{-14} \geqslant$

$C(\varepsilon \log N)^{-2}$ for a certain large enough C. Bounding again crudely $\log(2/v\widetilde{\alpha}) \ll$ $(\log 2v^{-1})(\log 2\widetilde{\alpha}^{-1})$ we also see that a sufficient condition for ω to satisfy (6.17) is

$$\omega \leqslant \exp\left(-C\alpha_1^{-1/2}(\log 2v^{-1})^2(\log 2\widetilde{\alpha}^{-1})^6\right)$$

which allows for the choice $\omega = N^{-(c\varepsilon/\log 2\widetilde{\alpha}^{-1})}$ upon inserting the above expression of $\log 2v^{-1}$. From Lemma 3.4 and the choices of v and ω we eventually obtain $\omega b_i^2 \geqslant N^{-\varepsilon}$ uniformly in $1 \leqslant i \leqslant n$. When we are in case (ii) of Proposition 6.6 we have therefore found the desired arithmetic progression. $\qquad\square$

7. Arithmetic progressions in sumsets of sets of primes

We now consider applications of Theorems 1.5 and 1.6 to the problem of finding arithmetic progressions in $A + A + A$, for A a subset of the primes. This problem was first considered by Cui, Li and Xue in [9]. In that paper a connection with the original problem on arithmetic progressions in sumsets of sets of integers was outlined and exploited via the original theorem of Green on $A+A+A$, which finds an arithmetic progression of size $N^{c\alpha^2}$ in this sumset when A has density α. To obtain Theorem 1.7 we exploit the same connection, taking advantage of the slightly longer progression given by Theorem 1.5. Corollary 1.8 is obtained differently, by a direct application of Theorem 1.6.

We denote by $\log_k$ the logarithm iterated k times and we let n be a large enough integer. We also recall that when G, H are two groups, a Freiman 3-isomorphism from $A \subset G$ to $B \subset H$ is a map $\phi\colon A \to B$ such that, for every $(a_i)_{1\leqslant i\leqslant 3}$ and $(a_i')_{1\leqslant i\leqslant 3}$ in A^3, $\sum_i a_i = \sum_i a_i'$ if and only if $\sum_i \phi(a_i) = \sum_i \phi(a_i')$; we refer to Section 5.3 of [24] for the properties of such maps. The following can be extracted from the computations of [9].

Proposition 7.1. *Let $\varepsilon, \delta \in (0,1)$ and suppose that A has density α in $\{1,\ldots,n\}\cap\mathcal{P}$. Then there exist an integer N such that $n/(\log n) \ll N \ll n$, a subset A' of A which is Freiman 3-isomorphic to a subset A'' of $\mathbb{Z}/N\mathbb{Z}$, a function f on $\mathbb{Z}/N\mathbb{Z}$ with support in A'' and a subset A_1 of $\mathbb{Z}/N\mathbb{Z}$ of density at least $c\alpha$ such that*

$$(7.1) \qquad f * f * f(x) \geqslant \alpha^3 \, 1_{A_1} * 1_{A_1} * 1_{A_1}(x) - O(\varepsilon + \delta^{1/2}) \qquad (x \in G)$$

provided $C(\log_4 N)/(\log_2 N) \leqslant (\varepsilon/2\pi)^{C\delta^{-5/2}}$.

Proposition 7.2. *Let $\varepsilon, \delta \in (0,1)$ and suppose that A has density α in $\{1,\ldots,n\}\cap\mathcal{P}$. Then there exist an integer N such that $n^{1/2} \ll N \ll n$, a subset A' of A which is Freiman 3-isomorphic to a subset A'' of $\mathbb{Z}/N\mathbb{Z}$, a function g on $\mathbb{Z}/N\mathbb{Z}$ with support in*

A'' and a subset A_1 of $\mathbb{Z}/N\mathbb{Z}$ of density at least $c\alpha^2$ such that

$$g * g * g(x) \geqslant \alpha^3 \, 1_{A_1} * 1_{A_1} * 1_{A_1}(x) - O(\varepsilon + \delta^{1/2}) \qquad (x \in G)$$

provided $\delta^{-5/2} \log 2\varepsilon^{-1} \leqslant c \log N$.

Proof of Theorem 1.7. To obtain the first estimate we apply Proposition 7.1. Since A_1 has density at least $c\alpha$ we know by Theorem 1.5 that $A_1 + A_1 + A_1$ contains an arithmetic progression P of length at least $N^{c\alpha/(\log 2\alpha^{-1})^5}$ such that, for every $x \in P$,

$$1_{A_1} * 1_{A_1} * 1_{A_1}(x) \geqslant \exp\left(-C\alpha^{-1}(\log 2\alpha^{-1})^7\right).$$

Choosing $\varepsilon = \delta = \exp(-C'\alpha^{-1}(\log 2\alpha^{-1})^7)$ with C' large enough it then follows from (7.1) that $f * f * f(x) > 0$ for all $x \in P$, and therefore that $P \subset A'' + A'' + A''$. Pulling back to $A' \subset A$ by the Freiman isomorphism we are done provided $\delta^{-5/2} \log 2\varepsilon^{-1} \leqslant c \log_3 N$, which is satisfied for $\alpha \geqslant C(\log_5 N)^7 / \log_4 N$.

To obtain the second estimate we apply Proposition 7.2, where this time A_1 has density at least $c\alpha^2$. Theorem 1.5 then yields a progression $P \subset A_1 + A_1 + A_1$ of length at least $N^{c\alpha^2/(\log 2\alpha^{-1})^5}$ such that

$$1_{A_1} * 1_{A_1} * 1_{A_1}(x) \geqslant \exp\left(-C\alpha^{-2}(\log 2\alpha^{-1})^7\right),$$

and choosing $\delta = \varepsilon = \exp(-C'\alpha^{-2}(\log 2\alpha^{-1})^7)$ we may conclude as before provided

$$e^{C\alpha^{-2}(\log 2\alpha^{-1})^7} \leqslant c \log N.$$

This is certainly satisfied for $\alpha \geqslant C(\log_3 N)^{7/2}/(\log_2 N)^{1/2}$. $\qquad\square$

Proof of Corollary 1.8. The projection $\pi \colon \mathbb{Z} \to \mathbb{Z}/6N\mathbb{Z}$ is a Freiman 3-isomorphism from $A \subset \{1, \dots, N\}$ to $A' := \pi(A)$ which preserves arithmetic progressions. Note that A' has density $\gg \alpha/\log N$ in $\mathbb{Z}/6N\mathbb{Z}$. Applying Theorem 1.6 with $A = B = C = A'$, $\varepsilon = 1/2$ and pulling back to $\mathbb{Z}$ then concludes the proof. $\qquad\square$

8. Remarks and conclusion

There is a strong parallel between the quantitative results one can obtain about arithmetic progressions in sumsets and on Roth's theorem by the density-increment strategy of [20]. Indeed the limitation in the range of density in both problems is similar. To see this, consider a subset A of $\mathbb{Z}/N\mathbb{Z}$ of density α. Sanders [20] then showed that when $\alpha \geqslant (\log N)^{-1+o(1)}$, there exists a non-trivial three-term arithmetic progression in A, which Bloom [1] generalized to show (in particular) that for $\alpha \geqslant (\log N)^{-2+o(1)}$, any translation-invariant equation in four variables has a non-trivial solution in A. By

comparison, the same density-increment strategy applied to our problem can be made to obtain a long progression in $A + A$ in the range $\alpha \geqslant (\log N)^{-1+o(1)}$ (although this is not pursued here, since the argument of [6] is simpler in this case) and by Theorem 1.6 it yields one in $A+A+A$ for $\alpha \geqslant (\log N)^{-2+o(1)}$. It is therefore likely that any improvement of this technique would result in a better density dependency in both problems.

References

1. T. Bloom, *Translation-invariant equations and the method of Sanders*, Bull. London Math. Soc. **44** (2012), no. 5, 1050–1067.

2. J. Bourgain, *On arithmetic progressions in sums of sets of integers*, A tribute to Paul Erdős, Cambridge Univ. Press, Cambridge, 1990, pp. 105–109.

3. _____, *On triples in arithmetic progression*, Geom. Funct. Anal. **9** (1999), no. 5, 968–984.

4. _____, *Roth's theorem on progressions revisited*, J. Anal. Math. **104** (2008), 155–192.

5. M.-C. Chang, *A polynomial bound in Freiman's theorem*, Duke Math. J. **113** (2002), no. 3, 399–419.

6. E. Croot, I. Laba, and O. Sisask, *Arithmetic progressions in sumsets and L^p-almost-periodicity*, preprint (2011), http://arxiv.org/abs/1103.6000.

7. E. Croot, I. Ruzsa, and T. Schoen, *Arithmetic progressions in sparse sumsets*, Combinatorial number theory, de Gruyter, Berlin, 2007, pp. 157–164.

8. E. Croot and O. Sisask, *A probabilistic technique for finding almost-periods of convolutions*, Geom. Funct. Anal. **20** (2010), no. 6, 1367–1396.

9. Z. Cui, H. Li, and B. Xue, *Long arithmetic progressions in $A + A + A$ with A a prime subset*, J. Number Theory **132** (2012), no. 7, 1572–1582.

10. G. A. Freiman, H. Halberstam, and I. Z. Ruzsa, *Integer sum sets containing long arithmetic progressions*, J. London Math. Soc. (2) **46** (1992), no. 2, 193–201.

11. B. Green, *Arithmetic progressions in sumsets*, Geom. Funct. Anal. **12** (2002), no. 3, 584–597.

12. _____, *Roth's theorem in the primes*, Ann. of Math. (2) **161** (2005), no. 3, 1609–1636.

13. B. Green and T. Tao, *An inverse theorem for the Gowers $U_3(G)$ norm*, Proc. Edinburgh Math. Soc. **51** (2008), no. 1, 73–153.

14. M. Hamel, N. Lyall, K. Thompson, and N. Walters, *Arithmetic structure in sparse difference sets*, J. Number Theory **130** (2010), no. 7, 1581–1589.

15. H. A. Helfgott and A. de Roton, *Improving Roth's theorem in the primes*, Int. Math. Res. Not. IMRN (2011), no. 4, 767–783.

16. K. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104–109.

17. I. Z. Ruzsa, *Arithmetic progressions in sumsets*, Acta Arith. **60** (1991), no. 2, 191–202.

18. T. Sanders, *Additive structure in sumsets*, Math. Proc. Cambridge Philos. Soc. **144** (2008), no. 2, 289–316.

19. _____, *Three-term arithmetic progressions and sumsets*, Proc. Edinburgh Math. Soc. **52** (2009), 211–233.

20. _____, *On Roth's theorem on progressions*, Ann. of Math. (2) **174** (2011), no. 1, 619–636.

21. _____, *On certain other sets of integers*, J. Anal. Math. **116** (2012), 53–82.

22. _____, *On the Bogolyubov-Ruzsa lemma*, Anal. PDE **5** (2012), no. 3, 627–655.

23. W. M. Schmidt, *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer, Berlin, 1980.

24. T. Tao and V.H. Vu, *Additive combinatorics*, Cambridge University Press, 2006.

DÉPARTEMENT DE MATHÉMATIQUES ET STATISTIQUES, UNIVERSITÉ DE MONTRÉAL, CP 6128 SUCC. CENTRE-VILLE, MONTRÉAL QC H3C 3J7, CANADA

Email address: henriot@dms.umontreal.ca